Deutscher Bundestag **Drucksache 19/1390**

19. Wahlperiode 23.03.2018

Kleine Anfrage

der Abgeordneten Andrej Hunko, Anke Domscheit-Berg, Dr. Petra Sitte, Doris Achelwilm, Simone Barrientos, Birke Bull-Bischoff, Brigitte Freihold, Nicole Gohlke, Norbert Müller (Potsdam), Zaklin Nastic, Sören Pellmann, Martina Renner, Eva-Maria Elisabeth Schreiber, Katrin Werner, Kathrin Vogler, Sabine Zimmermann (Zwickau) und der Fraktion DIE LINKE.

Kompromittierung deutscher Regierungsnetze

Am 28. Februar 2018 meldete die Deutschen Presse-Agentur (dpa), „ausländische Hacker" seien in den Informationsverbund des Bundes Berlin-Bonn (IVBB) eingedrungen („Innenministerium: Hacker griffen deutsches Regierungsnetz an", morgenpost.de vom 28. Februar 2018). Im Auswärtigen Amt habe es „einen entsprechenden Vorfall" gegeben, auch das Verteidigungsministerium sei betroffen. Den Hinweis auf die Kompromittierung hätten deutsche Geheimdienste nach Informationen des Senders rbb am 19. Dezember von einem „ausländischen Partner" erhalten („Von der Uni ins Ministerium?", tagesschau.de vom 2. März 2018). In der Bundespressekonferenz vom 2. März 2018 wurde hierzu gemutmaßt, dieser Dienst käme aus dem Baltikum („Regierungspressekonferenz vom 2. März 2018", bundesregierung.de). Nun ermitteln Bundesamt für Sicherheit in der Informationstechnik (BSI) und das für Spionageabwehr zuständige Bundesamt für Verfassungsschutz (BfV), auch der Auslandsgeheimdienst Bundesnachrichtendienst (BND) ist eingebunden. Verbindungsdaten des IVBB werden drei Monate aufgehoben. Für rund neun Monate der Angriffe stehen für die Ermittlungen deshalb keine Logfiles zur Verfügung.

Als Urheber des „Vorfalls" wurde von der dpa das in Russland verortete Netzwerk „APT28" benannt, das auch für Phishing-Mails an Bundestagsbüros im Jahr 2015 verantwortlich sein soll. Einen Tag später korrigierte sich die Agentur und schrieb den „Vorfall" unter Berufung auf ungenannte „Kreise" dem ebenfalls in Russland verorteten Netzwerk „Snake" zu, das „Verbindungen" zu russischen Geheimdiensten habe („Kreise: Russische „Snake"-Hacker hinter Angriff", dpa vom 1. März 2018). „Snake" ist eigentlich die Bezeichnung für die Schadsoftware „Turla" bzw. „Uroburos" (www.kaspersky.de/resource-center/threats/epic-turla-snake-malware-attacks), wird jedoch synonym zur Bezeichnung mutmaßlicher Angreifer gebraucht. Der Trojaner „Uroburos" wurde 2008 entdeckt und soll kyrillische Schriftzeichen im Programmcode enthalten, seit 2014 soll eine Linux-Variante kursieren (https://malwarebattle.blogspot.de/2014/03/g-data-found-russian-cyber-weapon.html). Sicherheitsfirmen wiesen in den vergangenen Jahren darauf hin, dass „Uroburos" Teil einer internationalen „Spionagekampagne" gewesen sei, die weltweit „Botschaften, Rüstungsfirmen, Lehranstalten und Forschungsinstitute" betroffen habe (https://securelist.com/the-epic-turla-operation/65545/). Auch im Bundesinnenministerium war dies bekannt. Im Verfassungsschutzbericht für 2016 heißt es, dass „Snake" seit 2005 mit der „sehr komplexen

und qualitativ hochwertigen Schadsoftware“ aktiv sei. „Uroburos“ sei darauf ausgelegt, „in großen Netzwerken von Behörden, Firmen und Forschungseinrichtungen zu agieren“. Betroffen seien insbesondere die Bereiche Energietechnik, Röntgen- und Nukleartechnologie, Messtechnologie sowie Luft- und Raumfahrt.

Das Rootkit „Uroburos“, das sich selbstständig in infizierten Netzwerken verbreitet, besteht aus zwei Dateien für 32- und 64-Bit-Windows-Systeme mit einem Treiber. Die Kompromittierung des IVBB sei laut der dpa über Computer einer Fachhochschule des Bundes für öffentliche Verwaltung erfolgt, Aktivitäten seien ab Ende 2016 festgestellt worden („Kreise: Russische ‚Snake‘-Hacker hinter Angriff“, dpa vom 1. März 2018). Der Angriff wurde möglicherweise durch fehlende Sicherheitsupdates oder eine großzügige Rechtevergabe begünstigt. Gewöhnlich nutzen Angreifer auch nicht veröffentlichte Sicherheitslücken („Zero Day Exploits“). Laut dem Verfassungsschutzbericht für 2016 erfolgten Infektionen mit „Uroburos“ meist über sogenannte Watering-Hole-Attacken, bei denen Angreifer Webpräsenzen, die für das Opfer potenziell interessant sind, auf infizierte Webserver umleiten. Werden die Seiten aufgerufen, erfolgt die Installation der Schadsoftware bei dem Opfer des Cyberangriffs. Die ausgewählten Betroffenen seien auf einer sogenannten White-List gespeichert. In der Süddeutschen Zeitung vom 6. März 2018 heißt es dazu, die Angreifer hätten das Mailprogramm Microsoft Outlook genutzt, um dort codierte Befehle in einem Mail-Anhang zu verstecken. Der betroffene Rechner war demnach bereits mit Schadsoftware infiziert. Über Outlook sollen die Dokumente schließlich auch ausgeleitet worden sein. Infiziert worden sei zunächst die Liegenschaftsverwaltung des Außenministeriums, danach ein Referat mit Russlandbezug. Im Januar 2017 habe die Malware einen Steuerbefehl erhalten und begonnen, Informationen an einen nicht näher benannten Server auszuleiten. Im März hätten die Angreifer dann Administrator-Rechte auf Windows-Clients im Auswärtigen Amt erlangt. Erst kurz vorher wurden die dortigen Linux-Systeme zu Windows und Microsoft migriert (Bundestagsdrucksache 18/4473). Einen der Rechner habe ein Mitarbeiter des Bundesverteidigungsministeriums genutzt. Das Verteidigungsministerium soll deshalb entgegen erster Informationen nicht direkt betroffen gewesen sein.

Der IT-Angriff hat nach derzeitigem Stand keinen großen Schaden angerichtet. Im IVBB werden keine vertraulich oder geheim eingestuften Dokumente verteilt („Regierungspressekonferenz vom 2. März 2018“, bundesregierung.de). Die Rede ist von sechs abgeflossenen Dokumenten, die zum Teil „Bezüge zu Russland, der Ukraine und Weißrussland“ hätten. Ein Mitarbeiter des Innenministeriums erklärte im Ausschuss für Verkehr und digitale Infrastruktur, das Parlament und die Öffentlichkeit sei nicht früher über den Vorfall informiert worden, um die Angreifer weiter beobachten und rückverfolgen zu können. Die an die Presse geleakten Informationen hätten die weitere Aufklärungsarbeit zwangsläufig beendet. Die Bundesanwaltschaft hat deshalb Vorermittlungen auf der Suche nach der undichten Stelle begonnen („Bundesanwaltschaft nimmt Vorermittlungen auf“, haz.de vom 2. März 2018). Nicht auszuschließen sei, dass die Veröffentlichungen dafür sorgten, dass die Angreifer Spuren löschen konnte.

In der Vergangenheit will die Bundesregierung täglich 20 „hoch spezialisierte Cyberangriffe“ festgestellt haben, von denen nach Einschätzung des BSI einer pro Woche „einen nachrichtendienstlichen Hintergrund“ gehabt hätte (Bundestagsdrucksache 18/11106, Frage 18). Für die Einstufung als „hoch spezialisierter Cyberangriff“ genügt es jedoch, wenn eine Schadsoftware die Virenscanner des BSI überwinden kann. In keinem der Fälle konnte der vermutete „nachrichtendienstliche Hintergrund“ bestätigt oder gar nachweislich einer Regierung zugeordnet werden.

Trotzdem will die Bundesregierung die rechtlichen und technischen Fähigkeiten zu digitalen Gegenschlägen ausweiten („Hacking back? Technische und politische Implikationen digitaler Gegenschläge“, SWP-Aktuell 59, August 2017). Der

Bundessicherheitsrat soll hierzu eine Analyse der benötigten technischen Fähigkeiten vornehmen und der Regierung Vorschläge für notwendige gesetzliche Änderungen vorlegen. Solche „Hackbacks“ könnten laut dem Chef der neuen Entschlüsselungsbehörde des Bundes (ZITiS) helfen, „entwendete Dateien und Dokumente zumindest auf den Servern der Diebe zu löschen“ („Entschlüsselungsbehörde - Staat muss digital zurückschlagen können“, de.reuters.com vom 22. November 2018). Auch im Koalitionsvertrag von Union und SPD heißt es, man wolle „Angriffe aus dem Cyberraum gegen unsere kritischen Infrastrukturen abwehren und verhindern“.

Wir fragen die Bundesregierung:

1. Wie viele „hoch spezialisierte Cyberangriffe“ stellt das BSI in 2016 und 2017 im Durchschnitt täglich im IVBB und im Bundestagsnetz fest, bei denen es als Einstufung genügte, dass die Virenscanner die Schadsoftware übersehen (Bundestagsdrucksache 18/11106, Frage 18)?
2. In wie vielen der Fälle wurde dabei ein „nachrichtendienstliche Hintergrund“ angenommen, und in wie vielen Fällen wurde dieser bestätigt oder gar nachweislich einer Regierung zugeordnet?
3. Welchem russischen Geheimdienst ordnet die Bundesregierung die „Cyberangriffskampagne APT 28“ zu (Bundestagsdrucksache 18/13667, Frage 12 des Abgeordneten Andrej Hunko)?
   a) Welche „Hinweise“ auf eine Spear-Phishing-Angriffswelle auf mehrere politische Parteien auf Bundes- und Landesebene wurden im August 2016 bekannt?
   b) Aus welchen Erwägungen oder nach welchen „Indizien“ wurden zurückliegende „Angriffsversuche“ dem Netzwerk „APT 28“ zugerechnet und welche „nachrichtendienstlichen Erkenntnisse“ lagen hierzu vor (Bundestagsdrucksache 18/11106, Frage 18; bitte die „Indizien“ ausführen)?
   c) Welche „Angriffsvorbereitungen“ konnten im Februar 2017 „erfolgreich verhindert werden“?
   d) Welche „Cyberangriffe“ erfolgte anschließend auf Netzwerke politischer Stiftungen und inwiefern handelte es sich dabei lediglich um den Versand von Spear-Phishing-Mails?
   e) Aus welchen Erwägungen oder nach welchen Indizien wurden diese Vorfälle von den deutschen Sicherheitsbehörden „als mögliche Vorbereitungshandlungen für Versuche einer Einflussnahme auf die Bundestagswahl angesehen“, die nach Kenntnis der Fragestellerinnen und Fragesteller schließlich nie erfolgte oder nachgewiesen werden konnte?
4. Handelt es sich bei dem jüngsten Angriff auf das deutsche Regierungsnetz nach Auffassung der Bundesregierung um einen Vorgang von besonderer Bedeutung gemäß §4 Absatz 1 PKGr und bitte begründen Sie diese Auffassung?

   Falls ja, wurde das PKGr umgehend unterrichtet oder wer entschied, vorerst von einer Unterrichtung abzusehen?

5. Welche IT-Systeme und welche Ministerien bzw. nachgelagerte Bundesbehörden waren von dem am 28. Februar 2018 bekannt gewordenen IT-Angriff nach derzeitigem Stand betroffen?

   a) Welche der dabei genutzten Angriffsinfrastruktur (insbesondere die Nutzung von Outlook und bekannter Server zum Ausleiten der Dokumente) ist bereits bei anderen Angriffen gegen Einrichtungen des Bundes festgestellt worden (Bundestagsdrucksache 18/11106, Frage 1)?

   b) Welche Schadsoftware wurde nach derzeitigem Stand bei dem Angriff genutzt?

   c) Wann und wo genau ist die Kompromittierung des IVBB erfolgt, und welchen Weg nahm die Schadsoftware?

   d) Inwiefern wurden bei dem Angriff nach derzeitigem Stand der Ermittlungen Webpräsenzen, die für das Opfer potenziell interessant sind, auf infizierte Webserver umgeleitet?

   e) Wann erhielten die Angreifer Administrator-Rechte auf den Web-Clients im Auswärtigen Amt?

   f) Wann erhielt die Schadsoftware einen Steuerbefehl und begann, Informationen auszuleiten, und welche Server wurden hierfür genutzt?

   g) Wann wurde der Angriff endgültig unter Kontrolle gebracht und die Schadsoftware aus dem IVBB entfernt?

      Ist die Bundesregierung sich sicher, dass die Schadsoftware vollständig entfernt wurde und kann ausschließen, dass sich Teile davon noch im IVBB Netz befinden?

   h) Für welchen Zeitraum werden im IVBB Vorratsdaten gespeichert und welche Logfiles des in Rede stehenden Angriffs stehen ab welchem Datum für Analysen und Ermittlungen zur Verfügung?

6. Inwiefern war das beim Bundesverwaltungsamt geführte und vom Bundeskriminalamt genutzte Passagierdatensystem in der Vergangenheit von IT-Sicherheitsvorfällen betroffen (bitte jeweils ausführen)?

   a) Aus welchen Gründen wurde das System wie berichtet abgeschaltet („Hacker sollen Dokumente zu Brexit und Ukraine entwendet haben“, zeit.de vom 10. März 2018, bitte mitteilen ob vorab nicht nur „Belastungstests“, sondern auch Penetrationstests durchgeführt wurden)?

   b) Welche Ergebnisse ergaben diese Tests jeweils mit Blick auf ihre Sicherheit?

7. In welchen Fällen war die Lernplattform „Ilias“, die an der Hochschule des Bundes zu Weiterbildungszwecken genutzt wird, in der Vergangenheit von IT-Sicherheitsvorfällen betroffen („Hack auf Bundesregierung erfolgte über Lernplattform Ilias“, golem.de vom 8. März 2018)?

   a) Kann die Bundesregierung bestätigen, dass der Standardaccount mit Administratorrechten mit dem Passwort „homer“ angelegt wurde?

   b) Wenn nein, welches war das Passwort bei der Erstanlage?

      Inwiefern kann die Bundesregierung sicherstellen, dass jedes dieser Initialpasswörter nach Installation sofort auf ein anderes Passwort geändert wurde?

   c) Inwiefern trifft es zu, dass „Ilias“ seit März 2017 in der Version 5.1.16 betrieben wurde, obwohl es danach mehrere Sicherheitsupdates gegeben hat?

   d) Welche Sicherheitslücken wurden durch die verzögerte Installation von Sicherheitsupdates ermöglicht (etwa Cross-Site-Scripting oder die Behandlung von Mediendateien)?

   e) Was ist der Bundesregierung darüber bekannt, wann genau die Version 5.1.16 eingespielt wurde und inwiefern der aktuelle IT-Sicherheitsvorfall davon profitierte, dass eine erst damit geschlossene Sicherheitslücke das Kopieren von Dateien an beliebige Stellen im Dateisystem ermöglichte?

8. Welche deutschen Geheimdienste oder Ministerien wurden wann von welchem „ausländischen Partner“, der möglicherweise aus dem Baltikum kommt, über den Angriff informiert?

9. Von welchen Ministerien, nachgelagerten Bundesbehörden oder Abteilungen wurde die Information über den laufenden Angriff nach derzeitigem Stand der Ermittlungen an die dpa weitergegeben, und inwiefern konnte die Bundesregierung analysieren, ob die Veröffentlichungen dafür sorgten, dass die Angreifer Spuren löschen konnten?

10. Welchen Schaden hat der Angriff nach derzeitigem Stand der Analyse angerichtet und welche Dokumente wurden kopiert?

    a) Welches „Referat mit Russlandbezug“ ist von dem Vorfall betroffen?

    b) Worin bestehen die „Bezüge zu Russland, der Ukraine und Weißrussland“, die den sechs kopierten Dokumenten zugeschrieben werden, und zu welchen weiteren Ländern hatten diese „Bezüge“?

11. Welche Bundesbehörden (auch die Bundesanwaltschaft) ermitteln zu dem Vorfall und damit im Zusammenhang stehenden Fragen, und wie sind die Zuständigkeiten geregelt?

12. Inwiefern kann die Bundesregierung die in den Medien vermutete Urheberschaft der in Russland verorteten Netzwerke „APT28“ oder „Snake“ bestätigen oder nicht bestätigen?

    Für wie sicher wird die Zuschreibung gehalten?

13. Welchem russischen Geheimdienst kann „Snake“ aus Sicht der Bundesregierung zugeordnet werden?

14. Seit wann ist dem Bundesinnenministerium der Trojaner „Uroburos“ bekannt und welche Vorkehrungen wurden für entsprechende Angriffe getroffen?

    a) Welche deutschen Netzwerke „von Behörden, Firmen und Forschungseinrichtungen“ wurden nach Kenntnis der Bundesregierung mit „Uroburos“ infiltriert bzw. welche Versuche sind hierzu bekannt (Verfassungsschutzbericht von 2016; sofern keine Details oder Zahlen der Angriffe mitgeteilt werden können, bitte deren Größenordnung angeben)?

    b) Aus welchen Quellen nimmt das BfV die Informationen, dass von „Uroburos“ bzw. „Snake“ insbesondere die Bereiche Energietechnik, Röntgen- und Nukleartechnologie, Messtechnologie sowie Luft- und Raumfahrt ausgeforscht würden?

    c) Welche technischen Details sind der Bundesregierung zur Software „Uroburos“ bekannt?

    d) Welche Dateisysteme kann „Uroburos“ infiltrieren, und wie verbreitet sich die Malware?

15. Inwiefern ist die von BfV und BND eingerichtete „temporäre Arbeitseinheit“ zur Prüfung, „ob die russische Regierung mit geheimdienstlichen Mitteln die politische Debatte und die öffentliche Meinung in Deutschland zu beeinflussen versucht“, weiterhin existent (Bundestagsdrucksache 18/10759, Frage 8)?

    a) Welche wesentlichen Ergebnisse schildert der Bericht, den die Bundesregierung beim BND und beim BfV zu vermeintlich russischen Aktivitäten im Cyberraum beauftragt hatte, zu denen es heißt die Bundesregierung habe diesen Bericht „zur Kenntnis genommen“ (Bundestagsdrucksache 18/11106, Frage 7)?

    b) Hinsichtlich welcher weiterer Regierungen außer den in der Beantwortung der Kleinen Anfragen auf Bundestagsdrucksachen 18/11106, 18/8631 und 18/10759 genannten Regierungen hat das BfV „Anwerbeversuche“ der „Mitarbeiter [deutscher] Parlamentarier oder politischer Stiftungen“ beobachten können?

16. Inwiefern könnte der am 28. Februar bekannt gewordene Angriff nach derzeitigem Stand der Analyse durch fehlende Sicherheitsupdates oder eine großzügige Rechtevergabe begünstigt worden sein. und wie ist hierzu im Auswärtigen Amt verfahren worden?

17. Inwiefern hätte der Angriff nach derzeitigem Stand der Analyse verhindert werden können, wenn das Auswärtige Amt nicht bis 2015 komplett auf Windows XP und Windows 7 umgestiegen wäre (Bundestagsdrucksache 18/4473)?

18. Wie viele E-Mails, die Schadsoftware enthielten, wurden im IVBB in den Jahren 2016 und 2017 abgefangen?

19. Wie viele Verbindungen zu Webseiten, die Schadsoftware enthielten, wurden im IVBB in den Jahren 2016 und 2017 unterbunden?

20. Inwiefern könnten die Angreifer nach derzeitigem Stand der Analyse nicht veröffentlichte Sicherheitslücken („Zero Day Exploits“) genutzt haben, und inwiefern ist es dem BSI überhaupt möglich, hierzu am Ende der Analyse und Ermittlungen mit endgültiger Klarheit Aussagen zu treffen?

21. Was kann die Bundesregierung über den Fortgang eines deutschen Prozesses mitteilen, in den Überlegungen zur Nutzung von Schwachstellen (sogenannten Exploits bzw. Zero Day Exploits) durch Strafverfolgungsbehörden oder Geheimdienste münden sollen (Bundestagsdrucksache 18/13696, Frage 25 des Abgeordneten Andrej Hunko)?

    a) Welche Kriterien müssten aus Sicht der Bundesregierung beispielsweise erfüllt sein, damit entschieden würde, dass eine gefundene Schwachstelle lieber nicht durch die Behörden ausgenutzt wird, sondern die Hersteller und Betreiber der Systeme gewarnt werden, damit sie diese schließen können?

    b) Sofern die Meinungsbildung innerhalb der Bundesregierung hierzu immer noch nicht abgeschlossen ist, wann kann sie zur Frage möglicher „Stufen eines Prozesses“ und zu möglichen „Kriterien“ eine Aussage treffen?

22. Mit welchen russischen Behörden arbeiten welche Bundesbehörden im Bereich der Cybersicherheit oder der Abwehr von IT-Angriffen regelmäßig in technischen, operativen und strategischen Fragen zusammen?

23. Sofern der am 28. Februar bekanntgewordene Angriff einem Staat zugerechnet werden kann, nach welcher Maßgabe hätte die Bundesregierung aus ihrer Sicht das Recht, diesen für sein Fehlverhalten zu sanktionieren?

24. Aus welchen Erwägungen hält es die Bundesregierung für notwendig, die rechtlichen und technischen Fähigkeiten zu digitalen Gegenschlägen auszuweiten und welche Pläne wird sie hierzu verfolgen („Hacking back? Technische und politische Implikationen digitaler Gegenschläge“, SWP-Aktuell 59, August 2017)?

    a) Welche Ergebnisse kann die Bundesregierung zu Analysen der hierzu benötigten technischen Fähigkeiten mitteilen, und welche Vorschläge für notwendige gesetzliche Änderungen wurden hierzu ermittelt?

    b) Inwiefern sollten vor einem digitalen Gegenschlag zunächst internationale Rechtshilfeersuchen gestellt werden, um Angreifer zu ermitteln und die Behörden des zuständigen Landes zur Mitarbeit bei der Abwehr aufzufordern?

    c) Welche Behörden sollten aus Sicht der Bundesregierung mit Möglichkeiten digitaler Angriffe oder Gegenschläge ausgestattet werden?

    d) Über wie viele Mitarbeiterinnen und Mitarbeiter verfügt das vor einem Jahr bei der Bundeswehr gegründete Kommando „Cyber- und Informationsraum“, und welcher Personalbestand ist geplant?

    e) Auf welche Weise soll die Zusammenarbeit von Bund und Ländern bei der Cyberabwehr ausgebaut, verbessert und strukturell neu geordnet werden?

    f) Mit welchen Kompetenzen wird die Rolle des BSI diesbezüglich gestärkt und ist geplant, die Behörde unabhängig zu gestalten und die Nachordnung zum Bundesministerium des Innern aufzulösen, um Interessenskonflikte auszuschließen?

Berlin, den 16. März 2018

Dr. Sahra Wagenknecht, Dr. Dietmar Bartsch und Fraktion



Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333